Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A validation protocol for determining whether an untrusted authentication chip is valid, or not, including the steps of:

generating a random number in a trusted authentication chip;

applying, in the trusted authentication chip, a keyed one way function to the random number using a first key from the trusted authentication chip to produce ~~an~~ first encrypted outcome~~, in both the trusted authentication chip and an untrusted authentication chip~~;

applying, in the untrusted authentication chip, a keyed one way function to the random number using a second key from the untrusted authentication chip to produce a second encrypted outcome;

comparing the first encrypted outcome and the second encrypted outcome, without knowledge of the first key or the second key, ~~s produced in both the trusted and untrusted chips,~~ and in the event of a match considering the untrusted chip to be valid;

otherwise considering the untrusted chip to be invalid.

2. (Currently amended) A validation protocol according to claim 1, where the first and second keys ~~is~~ are kept secret.

3. (Original) A validation protocol according to claim 1, where the domain of the random numbers generated is non-deterministic.

4. (Original) A validation protocol according to claim 1, where the keyed one-way function is a symmetric cryptograph, a random number sequence, or a message authentication code.

5. (Currently amended) A validation protocol according to claim 1, where the first and second keys ~~has~~ have a minimum size of 128 bits where the one-way function is a symmetric cryptographic function.

6. (Currently Amended) A validation system for determining whether an untrusted

authentication is valid, or not, where the system comprises:

a random number generator to generate a random number;

a trusted authentication chip, the trusted authentication chip including a keyed one-way function and a first key for the one-way function, the trusted authentication chip applying the keyed one way function to the random number using the first key to produce a first encrypted outcome;

an untrusted authentication chip, the untrusted authentication chip including the keyed one way function and ~~the~~ a second key, the untrusted authentication chip applying the keyed one way function to the random number using the second key to produce a second encrypted outcome; and

comparison means to compare the first encrypted outcome and the second encrypted outcome, without knowledge of the first key or the second key~~outcomes produced in both the trusted and the untrusted chips when the keyed one-way function is applied to the random number in both the trusted chip and the untrusted chip~~;

whereby, in the event of a match between the outcomes from the trusted chip and the untrusted chip, the untrusted chip is considered to be valid.

7. (Currently amended) A validation system according to claim 6, where the first and second keys ~~is~~ are kept secret.

8. (Original) A validation system according to claim 6, where the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every random number is produced so that the next random number will be produced from a new seed.

9. (Original) A validation system according to claim 7, where each trusted authentication chip contains a random function to produce random numbers from a seed, and for a group of authentication chips, each chip has a different initial seed, so that the first call to each chip requesting a random number will produce different results for each chip in the group.

10. (Original) A validation system according to claim 8, where the domain of the random numbers generated is non-deterministic.

11. (Original) A validation system according to claim 6, where the keyed one-way functions is a symmetric cryptograph, a random number sequence, or a message authentication code.

12. (Currently amended) A validation system according to claim 6, where the first or second keys for the keyed one-way function ~~has~~ have at least 128 bits where the one-way function is a symmetric cryptographic function.